EXHIBIT B

Joint Opp to Class Cert Mot

Christopher Chorba (SBN 216692)
Ashley Rogers (SBN 286252)
Lauren M. Blas (SBN 296823)
Joseph R. Rose (SBN 279092)
Abigail A. Barrera (SBN 301746)
GIBSON, DUNN & CRUTCHER LLP
Counsel for Defendant Meta Platforms, Inc. (formerly known as Facebook, Inc.)

Brenda R. Sharton (*pro hac vice*)
Benjamin M. Sadun (SBN 287533)
Theodore E. Yale (*pro hac vice*)
DECHERT LLP
Counsel for Defendant Flo Health, Inc.

Benedict Y. Hur (SBN 224018)
Simona Agnolucci (SBN 246943)
Eduardo E. Santacana (SBN 281668)
Tiffany Lin (SBN 321472)
Yuhan Alice Chi (SBN 324072)
Argemira Flórez (SBN 331153)
WILLKIE FARR & GALLAGHER LLP
Counsel for Defendant Google LLC

Ann Marie Mortimer (SBN 169077)
Jason J. Kim (SBN 221476)
John J. Delionado (*pro hac vice*)
Samuel A. Danon (*pro hac vice*)
HUNTON ANDREWS KURTH LLP
Counsel for Defendant Flurry, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ERICA FRASCO, et al.,

Plaintiffs,

v.

FLO HEALTH, INC., GOOGLE LLC, FACEBOOK, INC., and FLURRY, INC.,

Defendants.

CASE NO. 3:21-cv-00757-JD (consolidated)

DEFENDANTS' JOINT OPPOSITION TO PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

Judge: Hon. James Donato
Court: Courtroom 11 - 19th Floor
Date: November 21, 2024
Time: 10:00 a.m.

DOCUMENT FILED UNDER SEAL PURSUANT TO LOCAL RULE 79-5

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

INTRODUCTION

The Court should deny the motion for class certification because there is no manageable way to try, for millions of Flo app users at a single stroke, plaintiffs' assortment of complex constitutional, common-law, and statutory privacy claims. Plaintiffs have not proposed a classwide method to resolve a host of individualized issues, including what users knew about the challenged data-sharing practices and when; what their devices did or did not send to Flurry, Google, and Meta; whether that information was allegedly health information; whether users treated any alleged health information sent as private; and where from and where to that information was sent. This case should not be a class action.

Flo, the developer of a period-tracking app, once used software-development kits (often called "SDKs") from Flurry, Google, and Meta to better understand and serve its users. According to plaintiffs, the Flo app used those SDKs to send information to Flurry, Google, and Meta about menstruation cycles, efforts to conceive, and pregnancies. But what Flurry, Google, and Meta actually received from the Flo app generally consisted of pseudonymous identifiers paired with binary values ("0" or "1") or text values (e.g., "known" or "unknown") that showed only ***whether*** information was entered into Flo's app, not ***what*** information was entered. Determining what limited information was sent from each device, and whether it could support plaintiffs' claims, turns on seven individualized issues—each of which is indispensable to defendants' constitutional right to test plaintiffs' claims and present their defenses—that predominate over any common issues and preclude certification. Courts have held each of these issues is reason enough to deny certification; together, they confirm that "common" issues do not predominate and that any class trial here would be hopelessly unmanageable.

First, there is no classwide method of determining whether a user's claims are timely. No case was filed within the one-year contractual limitations period, so users' claims are time-barred unless they did not discover the basis for their claim until shortly before this suit was filed. A class trial could not resolve whether and when each Flo app user learned about Flo's data-sharing practices. Many users learned about them years before any suit was filed. The challenged practices were old news—literally—by the time plaintiffs sued in 2021. The *Wall Street Journal* reported on the subject in early 2019, and over 100 other news outlets followed suit. As plaintiffs admitted in the complaint, hundreds of people commented on the *WSJ* article alone, and hundreds more wrote directly to Flo after the

article's publication. For them and the many others who read that news coverage, the limitations clock started ticking—and the deadline to file suit came and went. Plaintiffs, who bear the burden on this issue at both class certification and on the merits, have proposed no classwide method of eliminating from the class users who knew all about the challenged practices long before this suit was filed.

Second, a class trial will make it impossible to determine who knew about the challenged conduct yet continued to use the app anyway. Flo's policies stated it could share personal information from its users with other services, including the other defendants. And those defendants' policies also made clear they might collect personal information through products used by app developers. Plaintiffs have not proposed any classwide method of determining which Flo app users were fully aware of the alleged data sharing and consented through their continued use of the app.

Third, the proposed class includes only users who generated twelve specific "Custom Events" over the class period (November 2016 through February 2019). But it is impossible to determine on a classwide basis what information was sent for each user during that period. The device-level data sent to Google and Meta no longer exist, having been deleted under defendants' standard data-retention policies long before this case was filed; Flurry only has pseudonymized data; and Flo never had the data at all. Plaintiffs' inability to prove what was sent for each user matters because most of the information sent from the Flo app cannot be a basis for plaintiffs' claims. Most Custom Events show only *whether* information was entered into the Flo app, not *what* information was entered. Because there is no classwide method of determining what was sent for each class member, there is also no classwide method of showing what, if any, allegedly sensitive information was sent for each class member.

Fourth, plaintiffs have not proposed any classwide method to determine whether Flo app users treated the limited information transmitted to Flurry, Google, and Meta as private. If they did not—if, for example, they shared it publicly—they cannot recover large statutory damages when someone else disclosed it. For example, some plaintiffs posted about their menstrual cycles in real time on public social-media accounts. Others shared the same information with other period trackers that also sent information using SDKs. Determining whether other Flo app users did the same—or otherwise made clear they did not treat their information as private—would necessarily require individualized inquiries.

Fifth, plaintiffs have identified no common method to determine whether people who used the

Flo app entered information about themselves into the app or, if they did, that it was accurate. Because plaintiffs' claims depend entirely on the alleged sharing of personal "health" information, putative class members who entered inaccurate information, or information about other people, cannot possibly be injured. Many users are in that situation: For example, some who created Flo app accounts entered implausible ages (like "623"), and others gave other false information. Plaintiffs' own expert testified her husband deliberately entered inaccurate information into the app to "mess around with the data that may be getting analyzed." Plaintiffs have no way of weeding users like him out of the putative class.

Sixth, plaintiffs also have no classwide method of proving Flo app users suffered actual damages as a result of the practices challenged here—an issue that bears even on claims for statutory damages. Several plaintiffs admitted they did not suffer any damages. Determining which other Flo app users also suffered no actual harm would require as many trials as there are would-be class members.

Seventh, the statutory claim that carries the biggest monetary penalties—the California Invasion of Privacy Act (CIPA) claim—requires plaintiffs to prove information was sent from or received in *California*, but there is no way to prove that on a classwide basis either. The only data sharing that plaintiffs challenge here happened (if at all) when users took the survey necessary to use the app. But Californians travel a lot—and use apps everywhere. Meta and Google have data centers across the country, and Flurry has no data centers in California. Plaintiffs nowhere suggest any classwide method of screening out those who took the survey and whose information was received outside of California.

Plaintiffs have not proposed a way to answer *any* of these questions, much less all of them, on a classwide basis. And the only way to get around that problem would be to trample defendants' constitutional rights—by denying them the right to litigate their defenses to individual claims, *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 366-67 (2011), or by permitting Flo app users to recover damages even if they are uninjured and thus lack standing to sue, *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021). The Rules Enabling Act forbids that result. 28 U.S.C. § 2072(b) (no rule, including Rule 23, may "abridge, enlarge, or modify any substantive right"). So does the Due Process Clause. *See, e.g.*, *Lindsey v. Normet*, 405 U.S. 56, 66 (1972) ("'Due process requires that there be an opportunity to present every available defense.'").

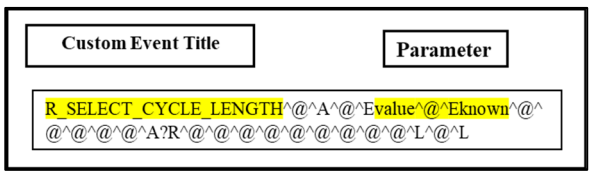
Finally, plaintiffs cannot possibly carry their burden to certify a class given the agreement each

user entered, *before entering the app*, that they would sue only on an individual basis. In other words, certification is precluded by the very contract plaintiffs are seeking to enforce. Literally everyone who installed the Flo app affirmatively accepted Flo's terms of service, which expressly bar users from "seek[ing] class treatment for any claim." The U.S. Supreme Court, the Ninth Circuit, and California courts have all affirmed class action waivers, and this Court should do the same. Having plaintiffs who believe they suffered actual harm bring claims individually, as they expressly agreed, is the right resolution—especially in light of all of individualized inquires necessitated here. The class-action waiver is dispositive for Flo.

FACTUAL BACKGROUND

Flo, like many other app developers, used SDKs offered by Flurry, Google, and Meta to understand how users interacted with its app and to improve its app's functionality. App. 941, 949, 954, 1603. These SDKs permit an app developer to send data about certain actions users take in its app to Flurry, Google, and Meta, which then return aggregated information about how users interact with the app. App. 952, 954-56.

Plaintiffs claim the Flo app sent to the other defendants, through SDKs embedded in the app, twelve "Custom Events" "that [allegedly] conveyed reproductive health information." Mot. 3. A Custom Event is a string of code that may include a title chosen by the app developer and optional parameters that convey data about in-app actions. App. 482, 880-81, 956-58. Parameters can be binary values (0 or 1), integers (e.g., 1, 5, or 7), or text values (e.g., "known" or "unknown"). App. 881-82, 1632-33. Consider the event "R_SELECT_CYCLE_LENGTH." Although the event's name suggests that this event conveyed the length of a user's menstrual cycle (in some number of days), that was not the case. In fact, the information the Flo app sent to Flurry, Google, and Meta showed only *whether* users knew their cycle length, not the actual length. Here's the string of characters Flurry, Google, and Meta supposedly received for that event:



Pls.' Ex. 5 at 70; *see also* App. 997-98, 1018-21, 1632-33. The event title and parameter were never

accompanied by any legend or decoder or any other context or explanation. App. 1605-06, 1380, 1431-32. The information sent was also tied not to a person, but to a device, via a user-resettable identifier consisting of a string of random numbers and letters. App. 961-64, 1077, 1610-13. People using the same device would appear to be a single user, and people could reset their identifiers (and appear as multiple users) or prevent them from being sent.

Plaintiffs claim that each of the twelve Custom Events at issue was sent, if at all, when someone on a particular device answered a series of questions as part of the app's "onboarding" survey. Mot. 3. The questions and potential answers in the survey changed during the class period, as did the Custom Events the app sent to Flurry, Google, and Meta. Pls.' Ex. 5 at 26, 23; App. 1373, 1381, 1632-33, 1666. The figure below illustrates some of the questions the Flo app asked people when they were setting up Flo accounts when the Flo app was first released. Underneath the questions are some of the Custom Event titles and parameters that plaintiffs claim were sent to Flurry, Google, and Meta:

Pls.' Ex. 5 at 26-27, ¶ 60.

The data Flurry, Google, and Meta received for a specific device depended on the user's responses to the questions in the onboarding survey and when the user took that survey. Pls.' Ex. 5 ¶¶ 97-99. Eleven of the twelve challenged Custom Events were not sent for every Flo app user. *See* App. 914 (observing that the "R_PREGNANCY_WEEK_CHOSEN" title was sent for less than 2 percent of plaintiffs' estimate of would-be class members). Consider, for example, plaintiff Tesha Gamino. She started using the Flo app in December 2016 and wanted to track her cycle. App. 116, 288-89. Flurry, Google, and Meta may have received a goal of "track_cycle"—along with parameters reflecting whether her last period date, period length, and cycle length were "known" or "unknown"—depending

on how she answered the onboarding survey questions. App. 1025-27, 1138, 1649-51. We do not know how she actually answered those questions. But her age would not have been sent because the Flo app did not send the Custom Event supposedly revealing age to Flurry, Google, or Meta until May 2018. Pls.' Ex. 5 ¶¶ 43, 69. And the Flo app also would not have sent any event with "Pregnancy" in the title because her goal was to track her cycle, not to track a pregnancy. App. 288-89.

There are no records showing which Custom Events Flurry, Google, or Meta received for any specific device, let alone a specific person. And because plaintiffs did not file this lawsuit until 2021, the device-level information received by Google and Meta no longer exists. Pls.' Ex. 38 at 14; App. 1244. Google and Meta have only aggregate records reflecting the Custom Event titles they received during the relevant period. App. 810-12, 814, 1195-209, 1244. And Flurry has only pseudonymized data. App. 1473. The evidence in the record about which of the twelve challenged Custom Events may have been sent for the named plaintiffs was developed based on discovery and testimony specific to each plaintiff, not on any of defendants' records.

LEGAL STANDARD

Rule 23 "imposes stringent requirements for certification that in practice exclude most claims." *Am. Express Co. v. Italian Colors Rest.*, 570 U.S. 228, 234 (2013). "[C]ertification is proper only if 'the trial court is satisfied, after a rigorous analysis'" based on evidence, not pleadings or speculation, that the plaintiff has met that burden. *Dukes*, 564 U.S. at 350-51.

STATEMENT OF ISSUE TO BE DECIDED UNDER RULE 7-4(a)(3)

Have plaintiffs carried their evidentiary burden to prove that each of the applicable Rule 23 requirements has been satisfied in this case?

ARGUMENT

I. Individualized Issues Predominate Over Common Issues

Plaintiffs bear the burden of demonstrating that "questions of law or fact common to class members predominate over any questions affecting only individual members." Fed. R. Civ. P. 23(b)(3). They have not carried that burden. They have failed to identify any classwide method of demonstrating each of seven issues essential to proving both Article III standing—an "indispensable part of the plaintiff's case" that "must be supported in the same way as any other" element, *Lujan v. Defs. of Wildlife*,

504 U.S. 555, 561 (1992)—and the merits of their claims: that (A) Flo app users' claims are timely; (B) users did not impliedly consent to the sharing of their information; (C) what was sent for each user could be considered health information; (D) users treated the information they entered into the Flo app as private; (E) users entered their own, real information; (F) they suffered actual damages as a result of defendants' conduct; and (G) their information was sent from or received in California. Each of those individualized issues would be reason enough not to certify the class; together, they demonstrate that even one individual trial on the pile of claims asserted by plaintiffs would be a lengthy and complex affair. A class trial would be an unmanageable mess.

A. Whether A Flo App User's Claims Are Timely Is An Individualized Issue

As this Court acknowledged at the outset of this case, the timeliness of Flo app users' claims "is going to be an issue" in this litigation and "is a non-trivial defense." Dkt. 154 at 23:13-17. The time to address that issue is now, and plaintiffs have not shown it can be done through common proof.

All of plaintiffs' claims are subject to the one-year limitations period in Flo's terms of service, App. 1531, 1538, which is enforceable, *Tompkins v. 23andMe, Inc.*, 840 F.3d 1016, 1032 (9th Cir. 2016).[1] Plaintiffs admit Flo stopped using the other defendants' SDKs in February 2019, yet plaintiffs did not file suit until 2021. Mot. 1; Dkt. 1. As a result, the claims of every plaintiff and would-be class member are presumptively untimely. Plaintiffs argue the limitations period should be "tolled by operation of the discovery rule." Dkt. 64 ¶ 243. But plaintiffs bear the burden to prove tolling at trial, *Anagnostellis v. Pitney Bowes Inc.*, 2013 WL 8840335, at *4 (C.D. Cal. Mar. 5, 2013), and they bear the burden of proving that defendants' limitations defense can be resolved on a classwide basis now, *Thorn v. Jefferson-Pilot Life Ins. Co.*, 445 F.3d 311 (4th Cir. 2006). Plaintiffs have not carried that burden, as there is no way to figure out who knew what, and when, without a mini-trial for each Flo app user. This is in large part because there are so many ways users could have learned about the challenged data-sharing practices more than a year before the complaint was filed. Here are just four:

(1) News articles specifically about the Flo app. As plaintiffs admit, many Flo app users cannot benefit from tolling because they learned about the data-sharing practices challenged here from

[1] In addition to that contractual limitations period, there are various other (short) statutory limitations periods—one year for CIPA, *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 134 (N.D. Cal. 2020), and two years for the common-law and constitutional privacy claims, Cal. Civ. Proc. Code § 335.1.

a "bombshell" 2019 *Wall Street Journal* article "exposing Flo Health's privacy violations." Dkt. 64 ¶¶ 124, 184, 267-69 (citing App. 688-94). The *WSJ* article was just the start. Other major news outlets published their own articles after the *WSJ*'s reporting, and would-be class members could also have learned about the alleged data sharing from seeing those articles. *E.g.*, App. 696-702.

These articles put anyone who read them on notice of the data sharing. For example, one *WSJ* reader lamented in the comments section the "[s]tunning revelations in this weekend's Journal about the extent to which third-party health and other personal apps are sharing real-time, personal data with Facebook via SDKs." App. 776. And as plaintiffs admit, hundreds of people complained directly to Flo. Dkt. 64 ¶ 184. In fact, more than 250 users emailed Flo's customer support just in the few weeks following the *WSJ* article's publication. App. 1477. One asked to delete her account "[b]ased on the recent news from the WSJ article," which had been published earlier that same day. App. 1548. Another said she was "disappointed to learn that Flo shares data with Facebook and other 3rd party apps." App. 1550. Plaintiffs quote similar protests in their complaint. *E.g.*, Dkt. 64 ¶ 268.

(2) New York investigation. Plaintiffs also acknowledge that, "following the *Wall Street Journal* publication," New York opened an investigation into Facebook concerning "data collection practices that included the collection of intimate health data from Flo Health users." Dkt. 64 ¶ 233. That investigation was opened at the direction of then-Governor Andrew Cuomo, in an order issued the same day the *WSJ* article was published. *E.g.*, App. 704-05. Even more would-be class members could have learned about the practices plaintiffs challenge through the reporting on this investigation.

(3) Defendants' disclosures. Class members also could have learned about the type of data shared via SDKs from any of the defendants' privacy policies and disclosures. App. 792-800, 803-05, 1212-61, 1309-27, 1484-85, 1509-11, 1514-25, 1528-39. For example, Flo's June 2016 privacy policy explained Flo "may share information, including [users'] personally identifying information" with third parties, "including . . . Facebook." App. 1510. And Flo's May 2018 privacy policy informed users that "[a]mong others we may share your Personal Data with . . . Facebook and Google . . . [and] Flurry." App. 1519-20. Several Meta policies disclosed that it receives information from third parties, matches it to users' accounts, and may serve ads based on that information. Meta's April 2018 "Data Policy," for instance, said Meta collects information from app developers through SDKs and may use it to

deliver ads, among other things. App. 794-95. Google's October 2017 privacy policy explained it collects information about "your activity on . . . apps" that "partner with Google to improve their content and services," including those that use "Google Analytics." App. 1228. Google's policies, terms, and Help Pages also specifically disclosed that it collects information from users of apps that use the Google Analytics for Firebase SDK, such as device identifiers, app-instance identifiers, IP addresses, and device event information. App. 1213, 1230, 1233, 1257.

(4) News articles and studies about period-tracking apps. Many Flo app users could have learned about the challenged data-sharing practices through publications about period-tracking apps that advised readers that sensitive information may be shared by those apps. App. 907-08. For example, in 2016, *The Washington Post* reported that many of the period-tracking apps used by millions of women "may have been leaking [users'] intimate information," including to advertising and analytics firms.[2] And in 2018, *Euronews* warned readers of "privacy tradeoffs" when using period-tracking apps, explaining that "[s]ome menstrual-cycle trackers share data with third parties without the users' consent while others ask for consent but don't specify which data will be shared."[3]

Investigative reports likewise informed readers that their information might be shared by health apps. For example, in 2013, the conclusion of an investigation of "43 popular health and fitness apps" was that "[c]onsumers should not assume any of their data is private in the mobile app environment—even health data that they consider sensitive." App 708-11. The report advised consumers to "[a]ssume any information [they] provide to an app may be distributed to the developer, third-party sites the developer uses for functionality, and unidentified third-party marketers and advertisers." *Id.*

Courts deny class certification if individualized questions about the statute of limitations would overwhelm the litigation. The Fourth Circuit, for example, affirmed the denial of class certification in a case about alleged racial disparities in insurance pricing because there was no classwide way of proving whether and when each would-be class member became aware of the pricing practices. *Thorn*, 445 F.3d 311. The court emphasized that the plaintiff "bears the burden" at class certification, including as to affirmative defenses. *Id.* at 322. Just as in *Thorn*, defendants' timeliness defense presents

[2] App. 730-32. The *Post* had a digital audience of 82.4 million people that month. App. 734.
[3] App. 737-43. In 2018, *Euronews* reached more than 430 million homes. App 745-47.

individualized questions about what each Flo app user knew and when, and plaintiffs have offered no classwide method of answering them. *See, e.g.*, *Broussard v. Meineke Disc. Muffler Shops, Inc.*, 155 F.3d 331, 342 (4th Cir. 1998) (reversing certification order in part because "tolling the statute of limitations on each of plaintiffs' claims depends on individualized showings"); *In re Kia Hyundai Vehicle Theft Litig.*, 2024 WL 2104571, at *7 (C.D. Cal. Apr. 22, 2024) ("statute of limitations will likely be at issue for a substantial number of insureds," which "weighs strongly against predominance").

B. Whether A Flo App User Implicitly Consented To Data Sharing Through Continued Use Is An Individualized Issue

Plaintiffs cannot prevail if they consented to Flo's sharing of Custom Event data with Flurry, Google, and Meta, because consent is a complete defense to all their claims. *See Brown v. Google*, 2022 WL 17961497, at *18-19 (N.D. Cal. Dec. 12, 2022) (implied consent is a defense to CIPA, California Comprehensive Computer Data Access and Fraud Act (CDAFA), invasion-of-privacy, intrusion-upon-seclusion, and breach-of-contract claims); *Brown v. Mortensen*, 51 Cal. 4th 1052, 1070 (2011) (Confidentiality of Medical Information Act (CMIA) permits disclosure of medical data with patient authorization); Cal. Penal Code § 502(c) (prohibiting certain conduct taken "without permission"). If app users knew about that data sharing but used the app anyway, they consented to it through their conduct and cannot press a claim: "courts in this district have found that users of applications implied consent through their conduct when they continued to use the applications despite exposure to materials that disclosed the challenged practices." *Hart v. TWC Prod. & Tech. LLC*, 2023 WL 3568078, at *10 (N.D. Cal. Mar. 30, 2023); *accord, e.g.*, *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 (N.D. Cal. Mar. 18, 2014). Here, users could have learned (and many did learn) about the challenged data sharing in many ways. *See supra* at pp. 7-9. And as this Court observed, "the scope of plaintiffs' consent" based on "different portions of [Flo's] various privacy policies over the years" involves "factual disputes" that a jury will have to resolve. Dkt. 485 at 3-4.

Courts regularly refuse to certify classes when it will be impossible to adjudicate implied consent on a classwide basis. Consider three examples. First, in *Brown*, the plaintiffs alleged Google "surreptitiously intercept[ed] and collect[ed] users' data even while users [we]re in a private browsing mode" known as "Incognito." 2022 WL 17961497, at *1. Google argued its "affirmative defense of

implied consent raise[d] individualized issues that defeat[ed] predominance," pointing to "media and academic reports that publicly disclosed the alleged conduct" and Google webpages explaining Incognito mode. *Id.* at *17-18. The court denied class certification, explaining that "Google provide[d] evidence that its consent defense would be based on individual, and subjective, interactions of what certain class members knew, read, saw, or encountered." *Id.* at *19.

Second, another court recently declined to certify a class because individualized inquiries were necessary to determine whether users of the Weather Channel app continued using it after learning that it might be recording and selling their location. *Hart*, 2023 WL 3568078, at *1, 10-11. The court explained that users could have learned about the defendant's alleged conduct from multiple sources, including the app's privacy policy and "a number of published news articles." *Id.* at *10-11.

Third, a court similarly denied certification of a class asserting wiretapping claims because individual inquiries were necessary to determine whether email users knew about and consented to Google's alleged interception of emails. *Gmail*, 2014 WL 1102660, at *17-18. There was a "panoply of sources from which email users" could have learned about the challenged practices, including Google's terms of service and news articles predating the plaintiffs' complaint. *Id.* at *17. Determining "to what disclosures each Class member was privy" and "whether that specific combination of disclosures was sufficient to imply consent" would "overwhelm any common questions." *Id.* at *18.

Here, too, individualized issues about what Flo app users knew and when they knew it would make it impossible to resolve defendants' implied-consent defense on a classwide basis.

C. Whether Alleged Health Data Were Shared Is An Individualized Issue

Even if plaintiffs' arguments had merit, all of their claims require them to prove Flurry, Google, and Meta received Custom Events revealing health information:

- **CMIA:** Plaintiffs must prove that Flo is "[a] provider of healthcare"—it is not—and "disclose[d] medical information regarding a patient." Cal. Civ. Code § 56.10.
- **Breach of contract:** Plaintiffs claim Flo breached its contract with users by sharing "users' actual health information," even though Flo supposedly "promised it would not do so." Mot. 11, 16; *see also* Dkt. 64 ¶ 292.
- **Invasion of privacy:** Plaintiffs claim they "had a reasonable expectation of privacy in their

intimate health data." Dkt. 64 ¶ 262; Mot. 17.[4]

- **CDAFA:** Plaintiffs claim transmissions from the Flo app to Flurry, Google, and Meta were "'without permission'" because Flo's privacy policy did not "disclose that Flo would share . . . Class Members' health data." Mot. 18; *see also* Dkt. 64 ¶¶ 417-18.
- **CIPA:** Plaintiffs contend Flurry, Google, and Meta unlawfully intercepted "Custom Events reflecting health information entered into the Flo app" because Flo's privacy policies "did not obtain consent to share health information." Mot. 21; *see also* Dkt. 64 ¶ 410.

Plaintiffs who cannot prove sensitive information was disclosed also lack standing. In privacy cases, courts decide whether a plaintiff has standing by looking to common-law privacy claims; Article III requires proof of a "concrete" injury, meaning "a harm[] traditionally recognized as providing a basis for a lawsuit in American courts," such as "disclosure of private information." *TransUnion*, 594 U.S. at 425-26 (cleaned up). Courts frequently dismiss claims for lack of standing where no sensitive information was shared. *See, e.g.*, *Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 724 (9th Cir. 2017) (affirming dismissal of invasion-of-privacy claim given failure to allege shared vehicle data were sensitive); *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5, 2023) (dismissing CIPA claim where plaintiff did "not allege that she disclosed any sensitive information").

The Court recently acknowledged that "whether the information [sent to] Google . . . contains private health information" turns on "questions of fact." Dkt. 485 at 2. The same is true for data sent to Flurry and Meta. These questions cannot be resolved on a classwide basis because whether health information was potentially shared about a Flo app user depends on what information was sent for that user—which varied based on each user's responses to the onboarding questions. Only some of the challenged Custom Events were sent for each user. App. 914. For example, R_PREGNANCY_WEEK_CHOSEN was sent for less than 2% of all Flo app users. App. 914. And most of the challenged Custom Events reflect only *whether* a user entered certain information. Pls.' Exs. 5 ¶ 69. For example, R_SELECT_LAST_PERIOD_DATE, R_SELECT_CYCLE_LENGTH, and R_SELECT_PERIOD_LENGTH were sent with data reflecting, at most, whether last period date, cycle length, and

[4] The Court granted summary judgment on the "aiding and abetting" invasion-of-privacy claim as to Google. Dkt. 485.

period length were "known" or "unknown." Pls.' Ex. 5 ¶¶ 60, 69, 86. Further, the Custom Events varied based on the version of the app and device used. App. 1373, 1381. As a result, the data that may have been shared with these Custom Event titles did not convey any health information.

There are no data that can be used to determine what Custom Events the Flo app sent to Flurry, Google, and Meta for *any* Flo app user over the class period. That lack of data results not from any misconduct, but from deletion under standard data-retention policies and/or the pseudonymization of the data, which defendants adopted to protect their users' privacy. App. 830, 807-12, 1244, 1473.

The only way the parties gained any sense of what information plaintiffs entered into the Flo app was through discovery. While discovery cannot conclusively prove what was sent, plaintiffs' own testimony confirms the variability in what *may* have been sent about users and shows that health data may not have been sent about many or all of them. For Ms. Gamino, for example, the Flo app may have sent her goal to track her cycle, along with data reflecting whether her last period date, period length, and cycle length were "known" or "unknown." Her age would not have been sent, nor would any of the challenged Events with "Pregnancy" in the title. App. 915, Pls.' Ex. 5 ¶¶ 43, 69. SESSION_CYCLE_DAY is the only other challenged Custom Event that may have been sent about Ms. Gamino, but there is no evidence about whether she (or any other user) selected "I don't remember" to the question "When did your last period start?" or whether she selected a date. This combination of data is also the most that may have been sent for Ms. Chen, Ms. Frasco, and Ms. Kiss. App. 915, Pls.' Ex. 5 ¶¶ 43, 69. None of the plaintiffs selected a goal to track a pregnancy, so no challenged Custom Event with "Pregnancy" in the title was shared about them. App. 915. For some or all of the plaintiffs, then, as well as at least a great many class members, it seems likely that *no* health information was shared.

Plaintiffs' only retort is that all Flo app users must have selected a goal in the onboarding survey, so at least R_CHOOSE_GOAL was shared about each of them. Mot. 6. But the selection of a "goal" is not enough to support plaintiffs' theory. The goal of tracking a cycle, for example, suggests only that the user may menstruate, but CMIA requires more—the disclosure of "medical information," defined as information "regarding a patient's medical history, mental health application information, reproductive or sexual health application information, mental or physical condition, or treatment." Cal. Civ. Code § 56.05(j). The mere fact that a woman might menstruate does not count as sensitive

"medical information." To the contrary, courts have warned against overreading the statute: "'It is clear from the plain meaning of the statute that medical information cannot mean just any patient-related information held by a health care provider.'" *Wilson v. Rater8, LLC*, 2021 WL 4865930, at *4 (S.D. Cal. Oct. 18, 2021). Instead, "medical information" must include "'substantive'" information relating to "'a patient's medical history, mental or physical condition, or treatment.'" *Id.* In *Wilson*, the court held that medical appointment and discharge information, among other things, do not count as "medical information," explaining that "information about the appointment cannot be said to constitute information regarding treatment." *Id.* at *4-5; *see also A.D. v. Aspen Dental Mgmt.*, 2024 WL 4119153, at *8 (N.D. Ill. Sept. 9, 2024). The same is true of a goal to track a cycle.

Under these circumstances, class certification should be denied. Rule 23 "requires a district court to determine whether individualized inquiries into th[e] standing issue would predominate over common questions," *Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC*, 31 F.4th 651, 668 n.12 (9th Cir. 2022) (en banc), and courts regularly deny certification, including in privacy cases, where "'it w[ould] be extraordinarily difficult to identify'" class members with standing. *Huber v. Simon's Agency, Inc.*, 84 F.4th 132, 157-58 (3d Cir. 2023). For example, in *Cordoba v. DIRECTV, LLC*, 942 F.3d 1259 (11th Cir. 2019), the Eleventh Circuit vacated certification of a TCPA class because it was likely "the individualized issue of standing will predominate over the common issues in the case." *Id.* at 1277. This Court should similarly deny class certification given the variability in whether any even arguably sensitive information was even disclosed for a given Flo app user.

Courts also routinely refuse to certify classes when plaintiffs fail to present evidence permitting classwide determination of a key threshold merits issue. Consider *Griffith v. TikTok, Inc.*, 2024 WL 4308813 (C.D. Cal. Sept. 9, 2024), which involved privacy claims challenging analytics technology offered by TikTok and incorporated into websites. As in this case, "the viability of Plaintiffs' claims depend[ed] on the nature of the information sent to Defendants," which varied based on the plaintiffs' activity on various websites. *Id.* at *4. And as in this case, "the existence of reasonable expectations of privacy and the requisite offensiveness . . . depend[ed] on the nature of the information collected from each class member." *Id.* at *6. The court held the "variation in information gathered . . . as to different class members" was "fatal to certification" because, among other problems, the class would

flunk the predominance requirement. *Id.* at *8. The court also emphasized that "the named Plaintiffs have not produced evidence of any data collected from them," and "it is not even clear that they have suffered any cognizable injury, while it appears that at least some class members may have." *Id.* at *9.

The same is true here. There is no common evidence that can be used to determine what information was shared about even the plaintiffs, much less all Flo app users. Without that evidence, there is no way of determining whether any alleged health information was shared about each user. Mini-trials would be required to figure out what each user selected in the initial survey—and therefore what data may have been sent to Flurry, Google, and Meta. This problem forecloses class certification.

D. Whether A Flo App User Treated Any Information Allegedly Sent To Flurry, Google, And Meta As Private Is An Individualized Issue

To have standing and prove her substantive claims, each plaintiff must prove that the information about her supposedly conveyed by the Custom Events sent by Flo to Flurry, Google, and Meta was private. Because the only way to figure out whether users treated their information as private is through mini-trials on each user's statements and conduct, the Court should not certify the class.

Flo app users who did not treat their information as private cannot prevail on plaintiffs' California constitutional, common-law, and statutory privacy claims:

- The constitutional and common-law claims require proof that Flo app users "conducted [themselves] in a manner consistent with an actual expectation of privacy." *Hill v. NCAA*, 7 Cal. 4th 1, 26 (1994); *accord, e.g.*, *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 933 n.5 (N.D. Cal. 2015).
- CMIA requires determining whether Flo app users "took measures to protect against the misuse of their information" and whether "third parties could have obtained this information through other means." *Vigil v. Muir Med. Grp. IPA, Inc.*, 84 Cal. App. 5th 197, 222 (2022). If Flo app users publicly shared their information, then they will not be able to establish that defendants' actions caused any resulting privacy harm. *Id.*
- And under CIPA, courts consider the "severity" and "extent of any intrusion into the plaintiff's privacy" from an alleged interception of data before awarding statutory damages; if Flo app users did not treat their data as private, there cannot have been any intrusion

warranting damages. *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 268-69 (N.D. Cal. 2016).

If Flo app users did not treat their information as private, they also lack Article III standing to sue over its disclosure. *Supra* at p. 12. Courts have entered judgment for defendants on privacy claims when the plaintiffs did not demonstrate they "considered [the disclosed] information . . . to be private." *Lyansky v. Coastal Carolina Univ.*, 2024 WL 3892540, at *15 (D.S.C. May 21, 2024); *see also I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022) ("'no liability for giving publicity to facts about the plaintiff's life that are matters of public record'"). The Supreme Court has similarly held that "[w]hat a person knowingly exposes to the public"—unlike what they "seek[] to preserve as private"—is not protected under the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 351 (1967).

Plaintiffs cannot prove, on a classwide basis, that each Flo user treated the information sent to Flurry, Google, and Meta as private. As the Ninth Circuit recently recognized, "the individual privacy interest implicated by a particular record may vary" because "not everyone may care to keep [all] medical or health [information] private." *Civ. Beat L. Ctr. for the Pub. Int., Inc. v. Maile*, 113 F.4th 1168, 1178-79 (9th Cir. 2024). And plaintiffs' testimony makes clear that, when it comes to the information at issue here, they have widely varying views on what counts as private.

Take, for example, the Custom Event "R_CHOOSE_GOAL." Between six and eight plaintiffs likely selected one of the three goals, "track my period." App. 915. Plaintiffs have different views on whether that goal is private. Two of them (Erica Frasco and Ms. Gamino) do not consider the fact that they menstruate to be private; others disagree with that view. App. 915. And that is just what plaintiffs *said*. What they *did*—and whether that conduct was consistent with what they said—also varied. For example, three plaintiffs (Ms. Frasco, Madeline Kiss, and Ms. Ridgway) shared menstruation-related information on their public social-media accounts, even though two of them (Ms. Kiss and Ms. Ridgway) testified they consider that type of information to be private. App. 888, 896-97, 905, 915. Ms. Chen and Ms. Meigs, by contrast, consider everything they entered into the Flo app to be "sensitive" information and did not share related information on social media. *See* App. 424-25, 899, 903, 915. But Ms. Chen, along with other plaintiffs, did not read Flo's terms of service or privacy policy before using the Flo app, which suggests she may not have cared, or did not care strongly, about keeping the information she entered into the Flo app private. *See* App. 427, 915, 1732-33.

Plaintiff	Stated Privacy Preference	Revealed Privacy Preference	
	Testified fact of menstruation is not private	Shared menstruation or pregnancy information publicly	Did not read Flo's terms or policies
Chen			X
Frasco	X	X	
Gamino	X		
Kiss		X	
Meigs			Cannot recall
Pietrzyk		X	X
Ridgway		X	X
Wellman		X	Cannot recall

Defendants were able to determine plaintiffs treated their information differently—and in some cases contrary to their theory of injury—only through plaintiff-specific discovery. The Court should not certify the class on the premise that defendants will not be able to uncover similar information about the millions of other class members—which could be done only on an individual basis. *See, e.g.*, *Dukes*, 564 U.S. at 367. Certification on those terms would sweep in large numbers of Flo app users who, because they did not treat any information that was shared as private, cannot have suffered any injury—and therefore would lack Article III standing to sue on their own.

Courts routinely deny certification in privacy cases when the issue of Article III standing presents individualized inquiries that would predominate over common ones. *See supra* at p. 14. In fact, a court recently denied certification because the plaintiffs failed to show the defendants "received sensitive information from all, or even most, class members," and it was "possible" that the vast majority of the class "suffered no cognizable harm." *Griffith*, 2024 WL 4308813, at *10.

Courts have declined to certify classes because, as in this case, resolution of the claims would turn on putative class members' individual privacy preferences. In *Hart*, weather-app users claimed the defendant collected their location data without their consent. 2023 WL 3568078, at *1. In denying certification, the court explained that resolving their privacy claim "turns on individualized factual questions of whether each user actually maintained their reasonable expectation of privacy." *Id.* at *9. A "'nonzero number'" of users may have known their location information was being collected, and those users had no reasonable expectation of privacy in using the app. *Id.* at *10-11; *see also, e.g.*, *In re Toll Roads Litig.*, 2018 WL 4952594, at *7 (C.D. Cal. July 31, 2018) (denying certification where

"[t]he reasonable expectation of privacy of class members . . . would turn on a slew of potential factors"); *Vigil*, 84 Cal. App. 5th at 222 (denying certification in CMIA case where question of "whether plaintiffs took measures to protect against the misuse of their information" was individualized).

The same is true here: there is no classwide method of proving Flo app users treated the information allegedly sent to Flurry, Google, and Meta as private.

E. Whether Personal Information Was Shared Is An Individualized Issue

Plaintiffs' claims all require proof that Flurry, Google, and Meta received information revealing plaintiffs' own personal information. "[B]oth the common law and the literal understandings of privacy encompass the individual's control of information *concerning his or her person*," *U.S. DOJ v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763-64 (1989) (emphasis added)—not information about other people or information that was fabricated. For that reason, a court recently dismissed a CMIA claim in a case similar to this one, *A.D. v. Aspen Dental Management, Inc.*, 2024 WL 4119153 (N.D. Ill. Sept. 9, 2024). There, the plaintiffs alleged that the defendant collected "protected health information" on its website and sent it to analytics companies like Meta. *Id.* at *1. In dismissing the plaintiffs' CMIA claim, the court explained that they had not alleged the information relayed to third parties was about *them*: "[a] person could very well search treatments, medical conditions, and potential providers for a partner, parent, or child," which does not "necessarily reveal[] information about *their* 'physical condition or treatment' as required by the CMIA." *Id.* at *8 (emphasis added).

Those who cannot prove their own information was disclosed also lack Article III standing to sue. The Supreme Court has emphasized plaintiffs may sue only over concrete harms *they* have suffered. *TransUnion*, 594 U.S. at 426-27; *Davis v. FEC*, 554 U.S. 724, 733-34 (2008). The Ninth Circuit affirmed the dismissal of an invasion-of-privacy claim because there were "no specific allegations" showing why vehicle data were "individually identifiable to particular drivers"; the plaintiffs therefore "failed to sufficiently allege an injury" that could satisfy Article III. *Cahen*, 717 F. App'x at 724. Post-*TransUnion*, courts regularly dismiss privacy cases because there was no disclosure of the plaintiff's own information—and therefore no "concrete harm that bears a close relationship to the substantive right of privacy." *Lightoller v. Jetblue Airways Corp.*, 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023); *see also, e.g.*, *Dinerstein v. Google, LLC*, 73 F.4th 502, 513 (7th Cir. 2023) (no standing to sue

over disclosure of "*anonymized* information"); *Mikulsky v. Noom, Inc.*, 2024 WL 251171, at *5 (S.D. Cal. Jan. 22, 2024) (similar). *Campbell v. Facebook*, 951 F.3d 1106 (9th Cir. 2020), which this Court suggested may have reached a contrary result, *see* Dkt. 485 at 3, was decided before *TransUnion* and did not address this issue. Instead, the court rejected the argument that the plaintiffs suffered no harm because their information was *later* anonymized when used. *See id.* at 1119.

There are many reasons why data associated with a device may not have been associated with a specific person, including because people may share devices or reset their device identifiers. App. 1635-36. In addition, many Flo app users entered fake data or data about someone else. For example, some users changed their date of birth in the app multiple times. Pls.' Ex. 1 at 20. Others said they were somewhere between 102 and 623 years old. App. 810, 1209. And, as Flo's Chief Product Officer testified, some users "click[ed] all the buttons" in the app to test it, rather than entering real information. App. 1501. And some users deliberately entered false information. For example, Plaintiffs' own expert, Dr. Golbeck, testified her husband used the Flo app and entered information that did not "correlate with any individual person's actual menstrual or fertility cycles." App. 470-71, 508, 512-13. His goal was "to mess around with the data"—which he started doing after watching a video encouraging people to "download period tracking apps" and enter fake information to hinder the enforcement of laws forbidding abortions after "the overturning of *Roe*." App. 470-71, 508-09. In addition, at least 15% of Flo app users were men, who might not have been entering their own, real information into the app. App. 1501-02, 1667. Plaintiffs cannot seek statutory damages on behalf of these users, yet they have not offered any classwide method (let alone a reliable one) for excluding such users from their lawsuit.[5]

In sum, plaintiffs have not demonstrated how they will prove that *all* Flo app users entered their own, accurate information—proof that is necessary to satisfy both Article III and plaintiffs' claims.

F. Whether A Flo App User Was Actually Harmed Is An Individualized Issue

Most of plaintiffs' claims also require proof of actual harm—that is, "some showing of damage

[5] This problem of fake data is not unique to Flo. Another of plaintiffs' experts, Mr. Hoffman, admitted that he and his students enter fake data into apps and websites, and that people often do so for "privacy" reasons. App. 499-501. He's right: in a 2021 study of U.S. consumers, "72% of . . . respondents say they sometimes provide fake personal information to access website content." App. 753; *accord, e.g.*, App. 768 (UK survey found "60% of consumers intentionally provide incorrect information when submitting their personal details online").

or loss[] *beyond* the mere invasion of statutory rights," such as loss of money or property, *In re Google Android Consumer Priv. Litig.*, 2013 WL 1283236, at *6 (N.D. Cal. Mar. 26, 2013) (emphasis added):

- "Under California law, a breach of contract claim requires a showing of . . . actual damage." *Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000).
- CDAFA plaintiffs must also prove they suffered "damage or loss by reason of a[n] [alleged] violation." Cal. Penal Code § 502(c)(e)(1). Courts have dismissed CDAFA claims because the plaintiffs "rel[ied] on intangible invasion of privacy allegations" to establish "damage or loss." *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1050 (N.D. Cal. 2018).
- And although CMIA and CIPA both provide that actual damages are not necessary to award statutory damages, courts must still consider *whether* there was any actual damage when awarding statutory damages. *See Campbell*, 315 F.R.D. at 268-69.

Here, plaintiffs argue they can prove harm beyond an intangible invasion of privacy rights on a classwide basis simply because one of their experts, Mr. Hoffman, says that the twelve Custom Events have some unquantified "financial value." Mot. 18-19. But he admitted he is not an expert in economics. App. 492. And it is far from clear that *any* plaintiff or Flo app user suffered any actual harm, and any assertion of actual harm would have to be tested individually. App. 878-79. Plaintiffs' depositions—which Mr. Hoffman did not review or consider—show why. App. 502-03. Some plaintiffs' testimony conclusively rebuts their own claims. Ms. Frasco, for example, admits she "cannot identify any harm" at all from the challenged conduct. App. 437. And although Justine Pietrzyk claims she "feel[s] violated" by the conduct, she admits she has not suffered any other type of harm. App. 455-56. Ms. Wellman says only that there is some "possibilit[y]" she suffered some additional harm beyond an "invasion of privacy." App. 337-38. In individual trials, defendants could secure admissions from other Flo app users that they suffered no actual, quantifiable harm—or, at the very least, could test through cross-examination vague assertions of actual harm like Ms. Wellman's. A class trial, by contrast, would deprive defendants of the right to test evidence showing whether any Flo app user was harmed in a way different from the supposed invasion of her statutory rights.

Courts routinely deny class certification where, as in this case, "[m]aking . . . a showing of actual harm on behalf of every class member is not feasible." *Duarte v. J.P. Morgan Chase Bank*, 2014

WL 12561052, at *3 (C.D. Cal. Apr. 7, 2014). For example, the Ninth Circuit concluded there was no classwide method of proving that an insurer had underpaid policyholders for their totaled cars. *Lara v. First Nat'l Ins. Co. of Am.*, 25 F.4th 1134 (9th Cir. 2022). Proving a supposed breach of an insurance regulation was not enough; the plaintiffs also had to prove actual underpayment, and "figuring out whether each plaintiff was injured would be an individualized process"—a bespoke valuation exercise. *Id.* at 1139-40. Similarly, in *Newton v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 259 F.3d 154 (3d Cir. 2001), investors sued their broker-dealers for failing to execute their trades at the best available price, even though, for some investors, no "better" price was available. *Id.* at 162, 178. The Third Circuit affirmed the denial of class certification, explaining that "determining actual injury would require hundreds of millions of individual assessments" into the availability of a "better" price. *Id.* at 187, 192. Those "individual issues overwhelmed common questions among the class." *Id.* at 187.

Courts have applied the same reasoning in the privacy context. In *Campbell*, for example, the court declined to certify a class of Facebook users seeking statutory damages under CIPA based on their allegation that Facebook "scan[ned] the content of their private [Facebook] messages" without their consent. 315 F.R.D. at 255. Explaining that "statutory damages are not to be awarded mechanically," the court identified six factors bearing on the decision to award such damages. *Id.* at 268. The court concluded that several factors "warrant[ed] individualized analyses," including, "critically, the question of 'whether or not there was actual damage to the plaintiff.'" *Id.* The court explained that "many class members appear[ed] to have suffered little, if any, harm," including one of the named plaintiffs, who testified that he was "not aware of any economic harm that he suffered." *Id.* at 268-69.

Another court recently denied certification in a data-breach case brought by an employee against her employer after it inadvertently disclosed its employees' W-2 statements to a third party. *McGlenn v. Driveline Retail Merchandising, Inc.*, 2021 WL 165121, at *10 (C.D. Ill. Jan. 19, 2021). The employer argued the plaintiff had "failed to prove that a substantial number of the class members have suffered actual injury"; there was no evidence the third party misused the disclosed information, or that employees had been hit with "bank charges," "service reinstatement fees," or "negative credit ratings." *Id.* at *9. The court held that the employer "ha[d] raised sufficient doubt" as to whether the "class members have actually suffered any injury," and that the plaintiff "ha[d] not presented sufficient

evidence that a number of class members have suffered a compensable injury." *Id.* at *10.

This case presents the same problem. Plaintiffs have no classwide evidence that Flo app users suffered actual harm. They have not offered any model that could show, on a classwide basis, whether and to what extent each user was harmed. Dkt. 431 at 1-2. Those evidentiary shortcomings make this case very different from the one on which plaintiffs rely, *Rodriguez v. Google LLC*, 2024 WL 38302 (N.D. Cal. Jan. 3, 2024). There, the plaintiffs' damages expert had provided "two models of unjust enrichment" capable of establishing "'damage or loss'" on a classwide basis. *Id.* at *6. Nor is this problem solved by the fact that plaintiffs seek, for instance, nominal and punitive damages. Even if there were "common" issues, there would be variability that precludes a finding of predominance, and the Court would still have to resolve this and the six other individualized issues *before* awarding any relief. *E.g.*, *Ang v. Bimbo Bakeries USA, Inc.*, 2018 WL 4181896, at *16 (N.D. Cal. Aug. 31, 2018).

In short, plaintiffs must prove actual harm to prevail on most of their claims, but the only way to do so, if at all, is on an individualized basis. The Court should therefore deny class certification.

G. Where A Flo App User's Data Were Sent or Received Is An Individualized Issue

A CIPA plaintiff must prove, among other things, that the defendant "read[], or attempt[ed] to read," a message while it was "in transit or passing over any wire, line or cable, or is being sent from, or received at any place within this state." Cal. Penal Code § 631(a). Plaintiffs contend that "[a]ll Flo app users must complete an onboarding survey the first time they use the app," and that all challenged Custom Events were sent to Flurry, Google, or Meta. Mot. 2-4. But plaintiffs have identified no classwide way to figure out whether those Custom Events were sent from or received in California.

That is because there is no such method. Flurry, Google, and Meta did not receive data only in California. Meta, for example, receives information from a device at a "Point of Presence," which functions like a cell tower. When people make phone calls, their cell phones usually connect to wireless networks through the nearest cell tower. Similarly, when information is transmitted from a device, it typically goes to the closest Point of Presence. App. 1170. So when a California resident uses an app outside of California, the Point of Presence that receives information from the app is also very likely to be outside of California. App. 1170. That happens a lot because, in the modern world, people are mobile. More than two million people travel just by air every single day. App. 780-90. And millions

of Californians live a short drive from Oregon, Nevada, Arizona, and Mexico.[6] Given the reality that Californians spend a lot of time outside of California, plaintiffs must show how they will prove with classwide evidence that *all* the putative class members sent *all* the challenged Custom Events to or from California. Plaintiffs have not done that. They do not account for the likelihood that a large share of the would-be class took the onboarding survey and generated Custom Events outside of California.

The same problem applies to plaintiffs' claims against Google and Flurry: Plaintiffs need, but do not have, a classwide method of proving Flo app users sent, or Google and Flurry received, the relevant information *in California*. For Google, analytics data are first transmitted to the closest available data collection center, encrypted, then forwarded to analytics processing servers. App. 1248, 1254. Google Analytics data can be processed at any data center, all of which are outside of California, or any Google Cloud Platform location, most of which are outside of California. App. 717-21, 773-74, 1254. And all of Flurry's servers are outside of California, App. 1473, so Flurry can be liable based only on where information was "sent from," not where it was "received." Cal. Penal Code § 631(a).

When, as in this case, a class member's location is essential to establishing a claim or defense, courts regularly hold that class certification is inappropriate. *See, e.g.*, *Hale v. Emerson Elec. Co.*, 942 F.3d 401, 402, 404 (8th Cir. 2019) (per curiam); *Spence v. Glock, Ges.m.b.H.*, 227 F.3d 308, 314-16 (5th Cir. 2000). Here, CIPA requires proof that all Flo app users took the onboarding survey in California or that their data were received there. But there is no classwide method of proving that.

II. The Court Should Not Certify An Injunctive-Relief Class

Plaintiffs tacked onto their motion a request for certification under Rule 23(b)(2), Mot. 24-25, but this case is a poor fit for that relief for four reasons. *First*, the seven individualized issues that bar any finding of predominance also bar any finding of commonality. *See, e.g.*, *Black Lives Matter L.A. v. City of Los Angeles*, 113 F.4th 1249, 1261 (9th Cir. 2024).

Second, the request is moot. Flo no longer uses the other defendants' SDKs, and there is nothing

[6] Unsurprisingly, plaintiffs testified they have spent time away from California—and thus may not have sent any data to Flurry, Google, or Meta from there. Ms. Kiss, for example, likely completed the onboarding survey outside of California. She originally downloaded the Flo app between "fall 2016" and "spring 2017," stopped using it, and then reinstalled it sometime in 2018. App. 393-94. But she lived in California only from February 2017 until June 2018. App. 389. It is possible she never even used the app while in California, let alone that any challenged Custom Events were sent from there.

suggesting the challenged practices will recur. *See, e.g.*, *Nelsen v. King Cnty.*, 895 F.2d 1248, 1254 (9th Cir. 1990); App. 1697, 1701. Flurry, Google, and Meta have data related to the twelve Custom Events only in an aggregated or pseudonymized form that is not being used for any purpose. App. 1191-92, 1273-74, 1697, 1701; *see supra* at p. 6. Where, as in this case, plaintiffs' requested injunctive relief is moot, it "cannot serve as a predicate for Rule 23(b)(2) certification." *Thorn*, 445 F.3d at 331; *accord, e.g.*, *Smith v. City of Oakland*, 2008 WL 2439691, at *1 (N.D. Cal. June 16, 2008).

Third, the injunction plaintiffs seek is disconnected from their claims. Plaintiffs want Flo to "delete all data relating to or derived from [their] pregnancy and menstruation information." Mot. 25. But this case has nothing to do with data Flo directly collects from its customers; it concerns only the challenged Custom Events Flo allegedly sent to Flurry, Google, and Meta. The whole point of using Flo's app is to track menstruation and pregnancies, so requiring Flo to delete all that information would render the app useless to its millions of users. Courts routinely hold injunctive relief is unavailable when the plaintiffs' requested relief has no connection to their claims. *E.g.*, *Pac. Radiation Oncology, LLC v. Queen's Med. Ctr.*, 810 F.3d 631, 637-38 (9th Cir. 2015); *Omega World Travel, Inc. v. Trans World Airlines*, 111 F.3d 14, 16 (4th Cir. 1997). The Court should do the same here.

Fourth, there is no need for an injunctive-relief class because this case is about money. "Rule 23(b)(2) certification is inappropriate where the primary relief sought is monetary." *Zinser v. Accufix Rsch. Inst., Inc.*, 253 F.3d 1180, 1195 (9th Cir. 2001). To determine the primary relief sought, the Court "has discretion to focus on [plaintiffs'] intent and whether monetary damages predominate over injunctive relief." *Broadbent v. Internet Direct Response*, 2011 WL 13217499, at *3 (C.D. Cal. Feb. 2, 2011). "Given the number of claims under which Plaintiffs seek damages," the many types of monetary damages sought, and the drive-by nature of plaintiffs' request for injunctive relief, "Plaintiffs' request for monetary damages is not merely incidental to the request for injunctive relief." *Id.* at *4; Dkt. 64.

III. Plaintiffs Are Contractually Barred From Bringing A Class Action

Everyone who entered the Flo app agreed to litigate "[a]ll claims between the parties . . . individually" and "not consolidate or seek class treatment for any claim." App. 1531, 1538. That agreement is enforceable. Courts decline to enforce class-action waivers only if (1) the plaintiffs did not receive "conspicuous notice," *Keebaugh v. Warner Bros. Ent. Inc.*, 100 F.4th 1005, 1013-14 (9th Cir.

2024), or (2) the waiver "is found in a consumer contract of adhesion in a setting in which disputes between the contracting parties predictably involve small amounts of damages, and . . . it is alleged that the party with the superior bargaining power has carried out a scheme to deliberately cheat large numbers of consumers out of individually small sums of money," *Discover Bank v. Super. Ct.*, 36 Cal. 4th 148, 162-63 (2005), *abrogated on other grounds by AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2011). Because Flo app users received notice and plaintiffs are not seeking small sums, it is axiomatic that they cannot circumvent their agreement to not bring class actions against Flo.

When people created Flo accounts, they either checked a box to confirm their agreement, App. 1563, or they saw a screen stating that "[b]y tapping 'Next,' you agree to the Terms of Use," App. 1558, which displayed a hyperlink to those terms in bold, underlined teal font near the button to create an account. Both sign-in screens provided conspicuous notice under California law. *See, e.g.*, *Berman v. Freedom Fin. Network, LLC*, 30 F.4th 849, 856 (9th Cir. 2022) (by "checking a box," user "manifests his or her assent to those terms"); *Oberstein v. Live Nation Ent., Inc.*, 60 F.4th 505, 516 (9th Cir. 2023) (notice "conspicuously displayed" when hyperlink is "distinguished from the surrounding text," such as by contrasting font and emphasized with borders outlining the hyperlinks).

Plaintiffs' motion also belies any assertion that this case concerns small amounts of money. Plaintiffs seek $1,000 *per violation* just for their CMIA claim. Mot. 21-22. And according to them, a CMIA violation occurred with *each* transmission of twelve Custom Events. Mot. 22. Under plaintiffs' theory, if a user triggered all twelve, that user could seek $12,000 in statutory damages for the CMIA claim alone—plus punitive damages—on the very first day of using the app. And of course, plaintiffs have asserted *thirteen* other claims. Dkt. 64 ¶¶ 259-425. Thus, this case does not concern a "small" sum of money. *See, e.g.*, *Math Magicians, Inc. v. Cap. for Merchs. LLC*, 2013 WL 6192559, at *9 (Cal. Ct. App, Nov. 26, 2013) (enforcing class waiver where plaintiff sought $18,000 in total); *Arguelles-Romero v. Super. Ct.*, 109 Cal. Rptr. 3d 289, 306 (2010) (same where plaintiff sought $16,000 in total). The class-action waiver is enforceable, and the Court should enforce it.

CONCLUSION

Because plaintiffs have not carried their evidentiary burden to prove that this case should be a class action, the Court should deny their motion.

Dated: October 3, 2024

/s/ Christopher Chorba
GIBSON, DUNN & CRUTCHER LLP
Christopher Chorba (SBN 216692)
CChorba@gibsondunn.com
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7396
Facsimile: 213.229.6396

Counsel for Defendant Meta Platforms, Inc.
(formerly known as Defendant Facebook, Inc.)

/s/ Brenda R. Sharton
DECHERT LLP
Brenda R. Sharton (*pro hac vice*)
One International Place
100 Oliver Street
Boston, MA 02110
Telephone: 617.728.7100
Facsimile: 617.426.6567
brenda.sharton@dechert.com

Benjamin M. Sadun
633 W 5th Street #4900
Los Angeles, CA 90071
Telephone: 617.728.7100
Facsimile: 617.426.6567
benjamin.sadun@dechert.com

Theodore E. Yale (*pro hac vice*)
2929 Arch Street
Philadelphia, PA 19104
Telephone: 215.994.4000
Facsimile: 215.655.2455
theodore.yale@dechert.com

Counsel for Defendant Flo Health, Inc.

/s/ Benedict Y. Hur
WILLKIE FARR & GALLAGHER LLP
Benedict Y. Hur (SBN 224018)
BHur@willkie.com
333 Bush Street, 34th Floor
San Francisco, CA 94104
Telephone: 415.858.7400
Facsimile: 415.858.7599

Counsel for Defendant Google LLC

/s/ *Jason J. Kim*
HUNTON ANDREWS KURTH LLP
Jason J. Kim (SBN 221476)
kimj@HuntonAK.com
550 S. Hope Street, Suite 2000
Los Angeles, CA 90071
Telephone: 213.532.2000
Facsimile: 213.532.2020

Counsel for Defendant Flurry, LLC

ATTESTATION (CIVIL LOCAL RULE 5-1(i)(3))

In accordance with Civil Local Rule 5-1(i)(3), I attest that concurrence in the filing of this document has been obtained from the signatories.

Dated: October 3, 2024

GIBSON, DUNN & CRUTCHER LLP

/s/ Christopher Chorba

Christopher Chorba